UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,338	09/17/2003	Yosef Stein	AD-356J	7044

7590 09/26/2007

Iandiorio & Teska
260 Bear Hill Road
Waltham, MA 02451-1018

EXAMINER	
POWERS, WILLIAM S	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/665,338	STEIN ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,12-14 and 29* is/are rejected.

7)☒ Claim(s) *2-11, 16-28, 30 and 31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 2 and 18 have been amended.

2. Claims 1- 31 are pending.

Response to Amendment

3. Applicant's arguments filed 7/16/2007 have been fully considered but they are not persuasive.

4. As to Applicant's argument that "the advanced encryption standard (AES) engine of the subject invention clearly should be given patentable weight because it produces 'a useful, concrete and tangible result'", the Examiner respectfully disagrees. The Applicant admits that the engine "may be implemented in software and/or hardware" (Remarks, page 11, lines 4-5). This makes the implementation of the engine software *per se*, which does not constitute one of the four statutory categories under 35 USC 101 (see MPEP 2106.01). For at least the reasons above, the 35 USC 101 rejection of the claims is maintained.

5. As to Applicant's argument that, McCanny's invention fails to disclose the applicant's claimed invention because it uses "one or more look-up table (LUTs) or ROMs", the Examiner respectfully disagrees. As pointed out by the Applicant, McCanny chose not to implement the subbyte transformation through "multiplicative inverse operation and affine transformation in logic" (Remarks, page 12, lines 9-10) because of cost and performance concerns. Clearly, McCanny was aware of using the multiplicative

inverse operation and affine transformation in the calculations and they could have been substituted if cost and performance had not been concerns. For at least the reasons above, the 35 USC 102 (e) rejection of the claims is maintained.

Response to Amendment

Claim Objections

6. In light of Applicant's amendment, the previous objection to claims 2 and 18 have been withdrawn.

7. Claim 1 objected to because of the following informality: the superscript of GF in line 5 is 1 and should be -1. Appropriate correction is required.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed invention is regarded as software *per se*. It is not tangibly embodied and, as such, is not classified under one of the four statutory categories.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 1, 12-15 and 29 are rejected under 35 U.S.C. 102(e) as being anticipated** by **McCanny et al. (2003/0039355 A1) cited in the IDS by Applicant.**

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

As per claim 1 McCanny et al. (2003/0039355 A1) disclose an advanced encryption standard (AES) engine with real time S-box generation comprising: a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^1(2^{m)}$ and applying an affine over GF(2) transformation to obtain a subbyte transformation (see

fig. 1a-c,3,5 and associated texts including item 32 of fig.3 and 54 of fig.5); and a shift register system for transforming said subbyte transformation to obtain a shift row transformation (see fig.2, item 32; fig.5, item 54 and associated texts); said Galois field multiplier system being responsive in a second mode to said shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of said first data block (see fig.4,5,5a,11 and associated texts in full). Also, see [0040-0062] and all other related paragraph.

As per claim 12 McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes at least one Galois field linear transformer and an associated polynomial multiplier (see fig.5 and associated texts; [0048-54]).

As per claim 13 McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes a reconfigurable matrix of cells (see fig.7 and associated texts).

As per claim 14 McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a key generator for providing a plurality of round keys (see fig.4 and associated text including round 0 to round final).

As per claim 14 McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 14 in which said key generator includes a key generator circuit responsive to a master key to generate said round keys (see fig.3-5 and associated text).

As per claim 29 McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a plurality of Galois field multiplier systems for simultaneously processing a plurality of subbytes (see fig.5 and associated text including item 54-58 where it disclose multiple subbytes).

Allowable Subject Matter

12. Claims 2-11, 16-28, 30 and 31 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

WSP

9/20/2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

William S. Powers
Examiner
Art Unit 2134